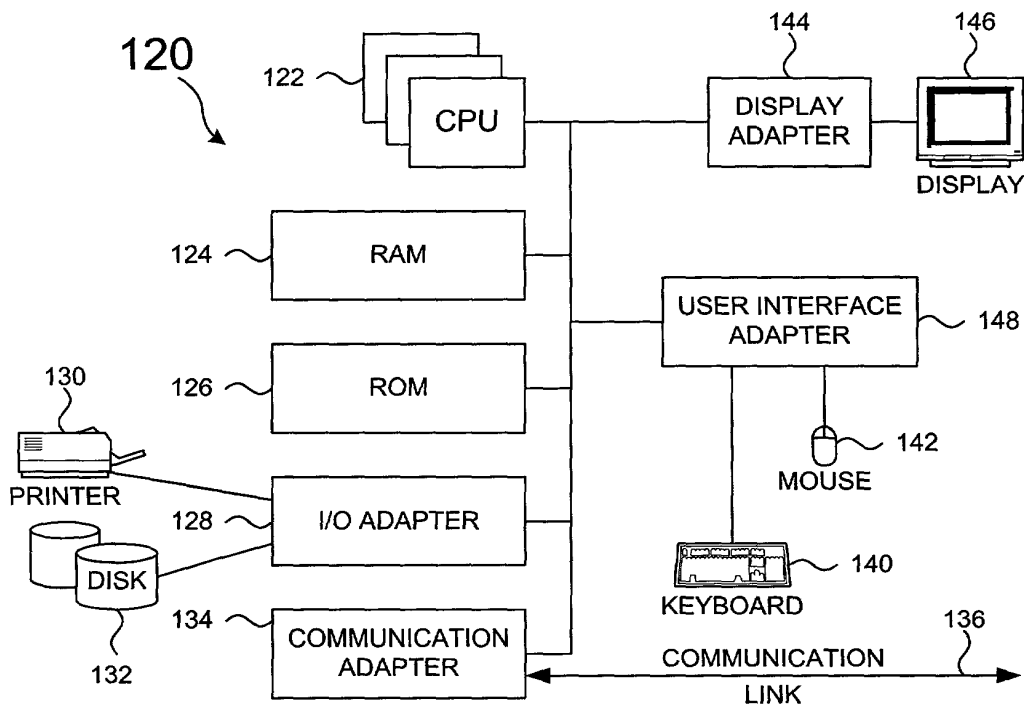
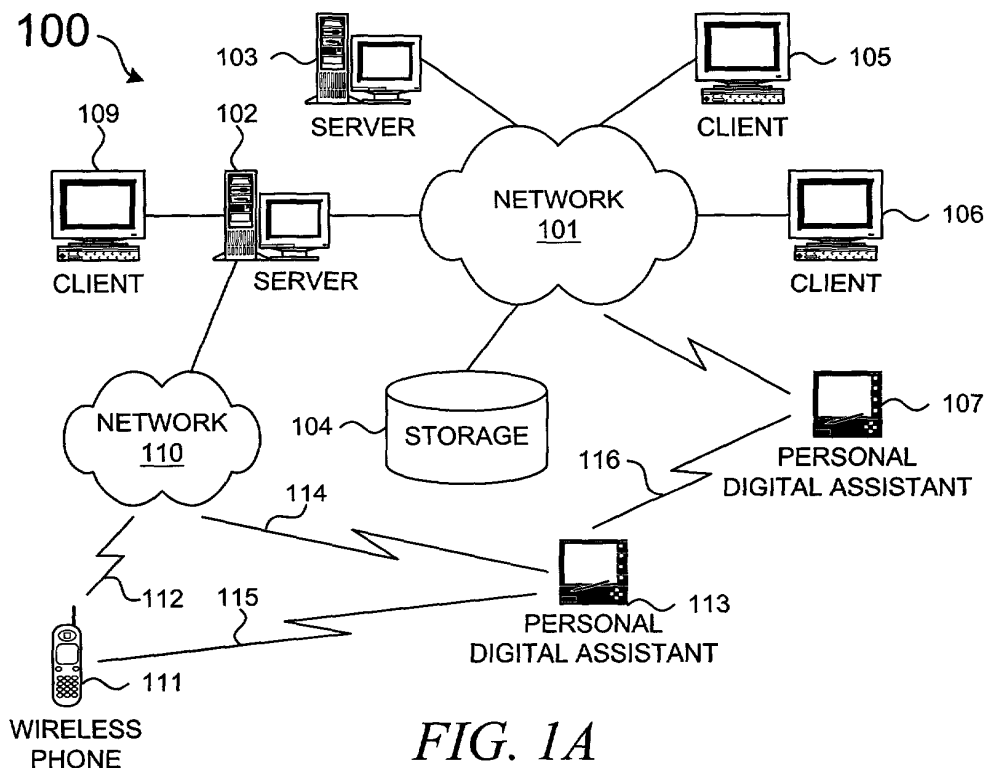


Method and system for a secure binding of a revoked X.509 certificate to
its corresponding certificate revocation list

1/6



Method and system for a secure binding of a revoked X.509 certificate to
its corresponding certificate revocation list

2/6

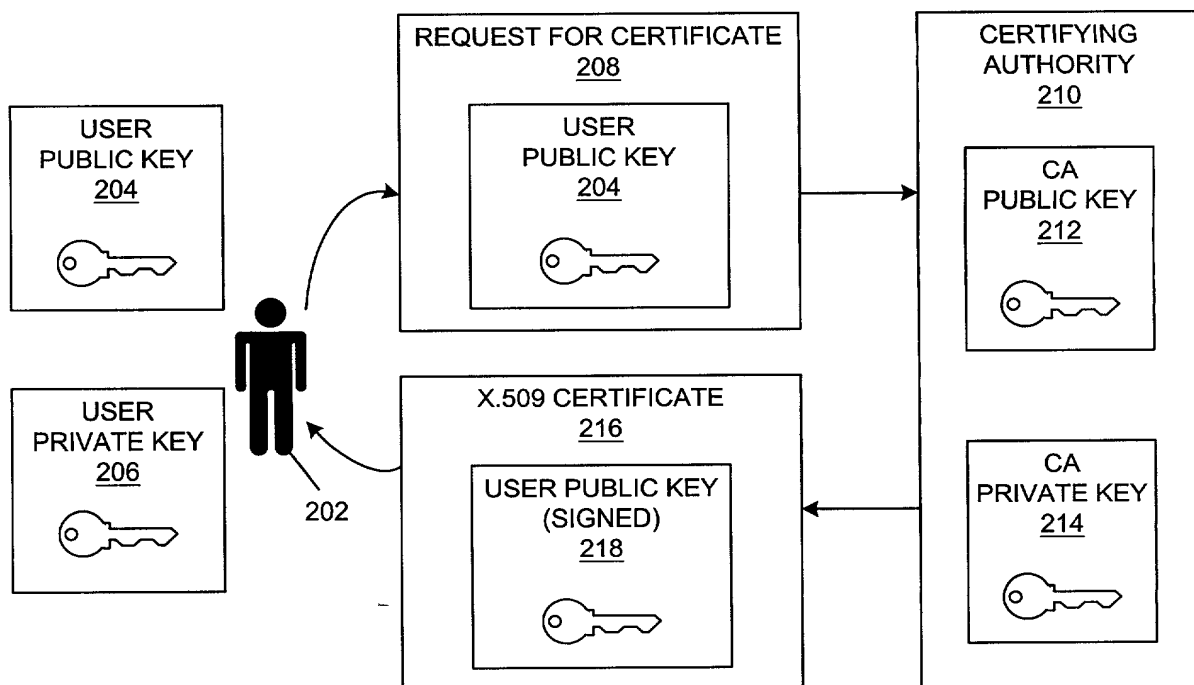


FIG. 2
(PRIOR ART)

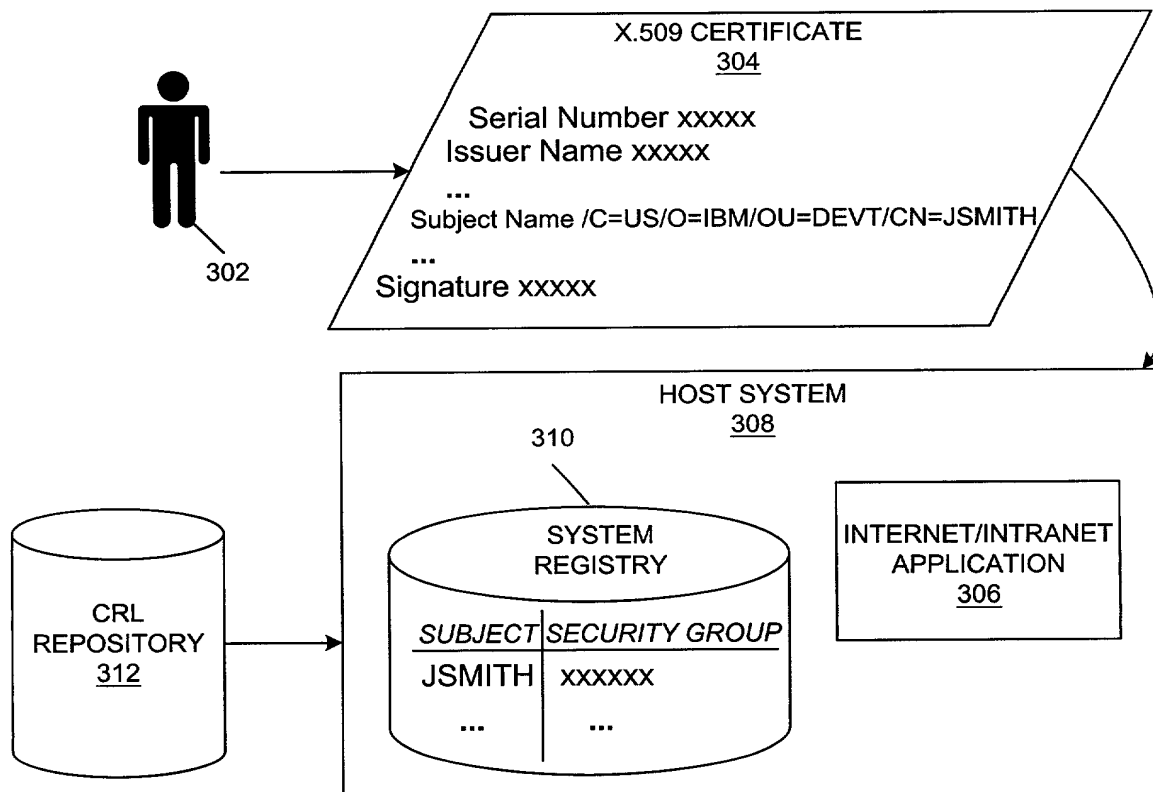


FIG. 3
(PRIOR ART)

3/6

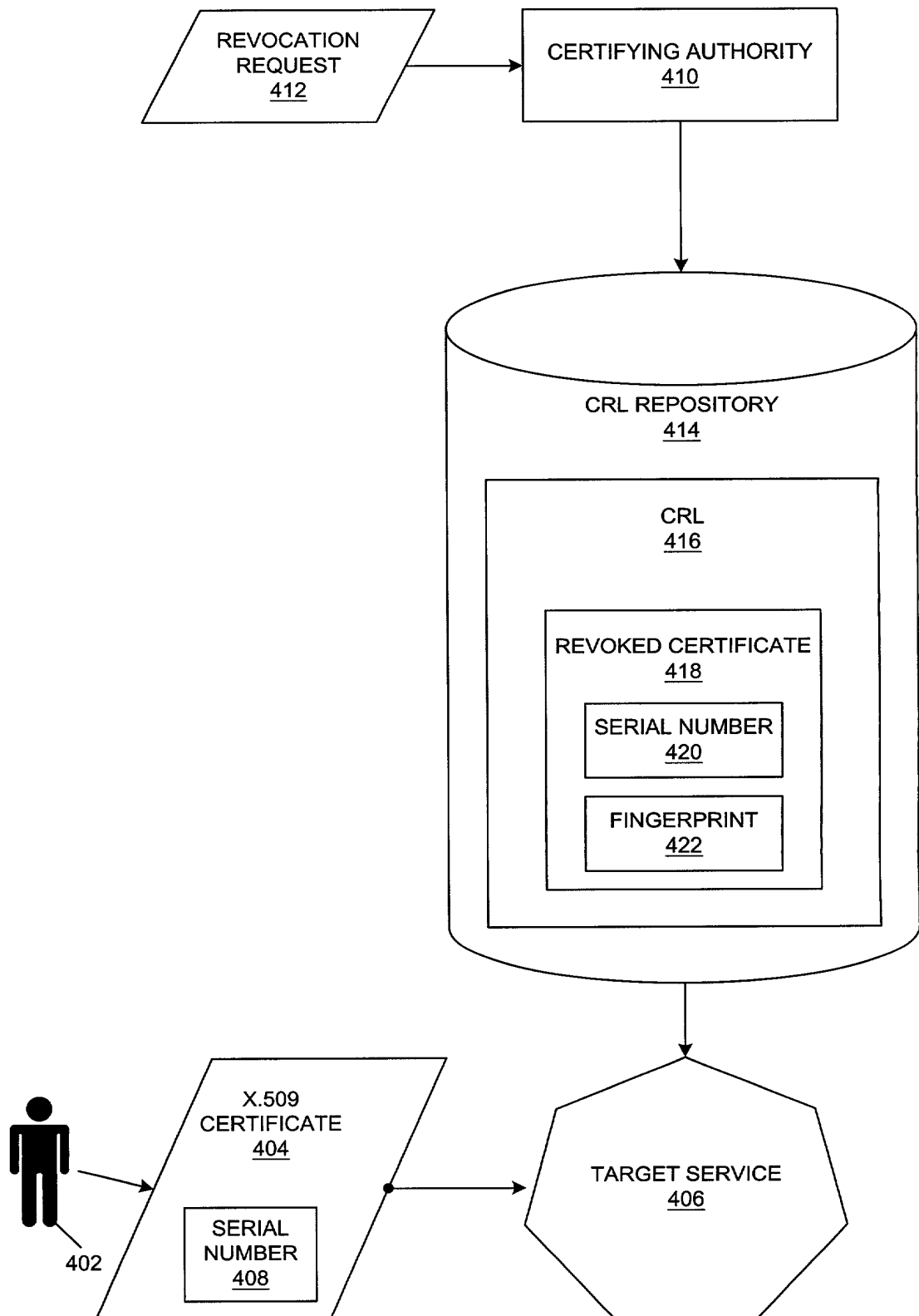


FIG. 4

4/6

Certificate ::= SEQUENCE {
 tbsCertificate TBSCertificate,
 signatureAlgorithm AlgorithmIdentifier,
 signature BIT STRING }

TBSCertificate ::= SEQUENCE {
 version [0] Version DEFAULT v1,
 serialNumber CertificateSerialNumber,
 signature AlgorithmIdentifier,
 issuer Name,
 validity Validity,
 subject Name,
 subjectPublicKeyInfo SubjectPublicKeyInfo,
 issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,
 subjectUniqueID [2] IMPLICIT UniqueIdentifier OPTIONAL,
 extensions [3] Extensions OPTIONAL }

Version ::= INTEGER { v1(0), v2(1), v3(2) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
 notBefore Time,
 notAfter Time }

Time ::= CHOICE {
 utcTime UTCTime,
 generalTime GeneralizedTime }

UniqueIdentifier ::= BIT STRING

SubjectPublicKeyInfo ::= SEQUENCE {
 algorithm AlgorithmIdentifier,
 subjectPublicKey BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
 extnID OBJECT IDENTIFIER,
 critical BOOLEAN DEFAULT FALSE,
 extnValue OCTET STRING }

FIG. 5A
(PRIOR ART)

Method and system for a secure binding of a revoked X.509 certificate to
its corresponding certificate revocation list

5/6

```
CertificateList ::= SEQUENCE {  
    tbsCertList      TBSCertList,  
    signatureAlgorithm AlgorithmIdentifier,  
    signatureValue    BIT STRING }  
  
TBSCertList ::= SEQUENCE {  
    version           Version OPTIONAL,  
    signature          AlgorithmIdentifier,  
    issuer             Name,  
    thisUpdate         Time,  
    nextUpdate         Time OPTIONAL,  
    revokedCertificates SEQUENCE OF SEQUENCE {  
        userCertificate CertificateSerialNumber,  
        revocationDate   Time,  
        crlEntryExtensions Extensions OPTIONAL  
    } OPTIONAL,  
    crlExtensions      [0] EXPLICIT Extensions OPTIONAL  
}
```

*FIG. 5B**(PRIOR ART)*

```
certFingerprint ::= SEQUENCE OF SEQUENCE {  
    algorithm      AlgorithmIdentifier,  
    fingerprint    octet string  
}
```

FIG. 6

6/6

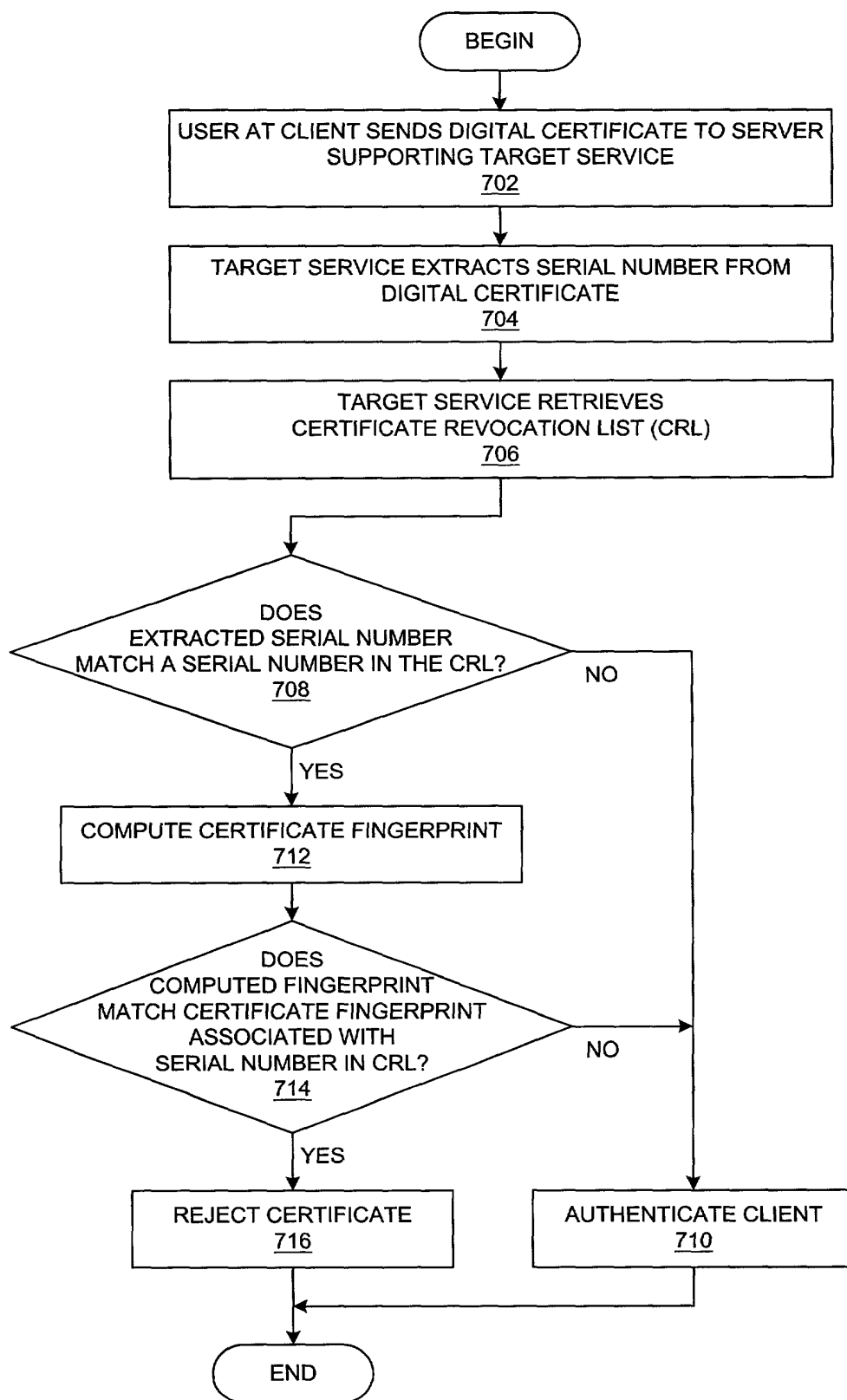


FIG. 7